Cybersecurity Strategy the National Security Aligning to EO14028

Shawn Kingsberry, SAIC, VP Cybersecurity

SAIC®

Cybersecurity Strategy the National Security aligning to EO14028

Recent events that transpired in 2022, such as the SolarWinds and Log4j exploitations, changed how the US Government views cybersecurity. On May 12, 2022, Executive Order 14028 was enacted, defining cybersecurity as now national security. The strategy for Information Technology has drastically shifted to blend digital transformation to cyber lead information technology modernization. This session describes the current threat the government is facing, and the high-level strategy laid out in the various executive orders, coupled with recommendations to build cyber strategies, Zero Trust Requirements, with technology examples as accelerators to drive benefit realization.

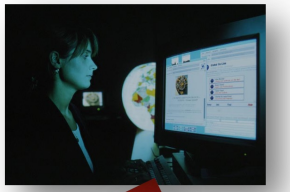
Humans Have Always Desired Connecting

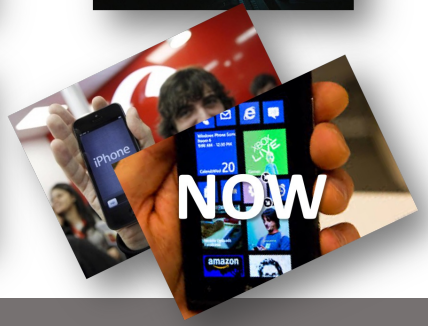
1962, a computer pioneer said,
"There is no reason to suppose the average boy or girl cannot be master of a personal computer."
Soon after, PCs arrived and have kept changing and changing.



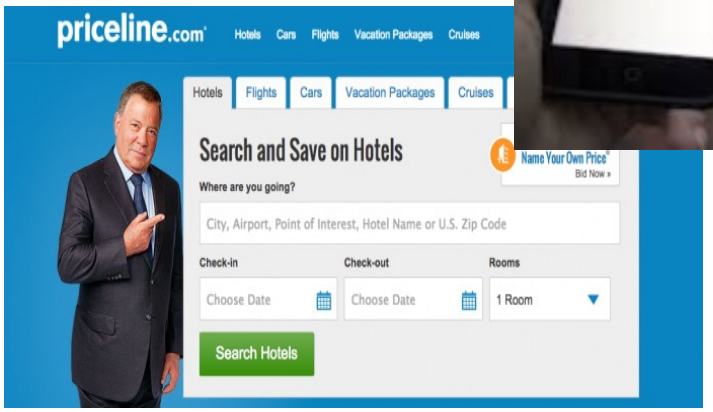




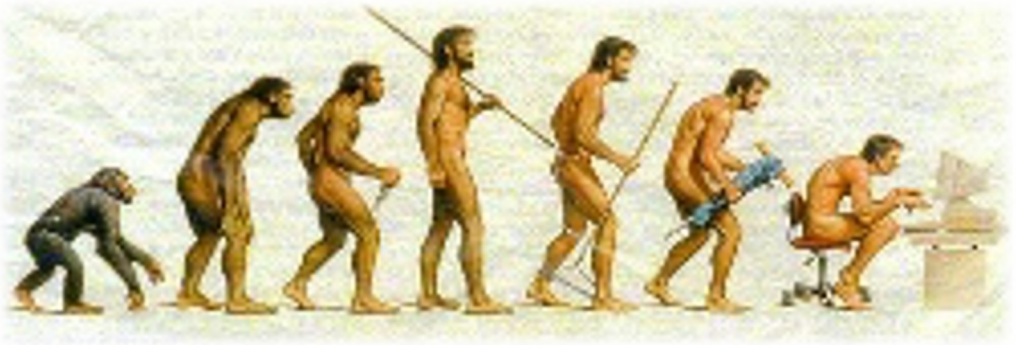


Technology Disrupting Traditional Industries and Markets

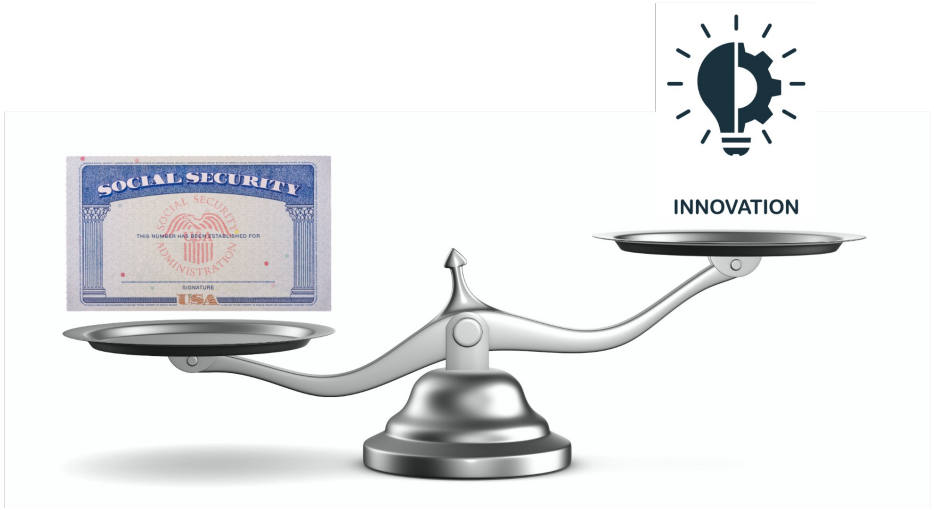


Evolution - The Digital Journey is Real



TO

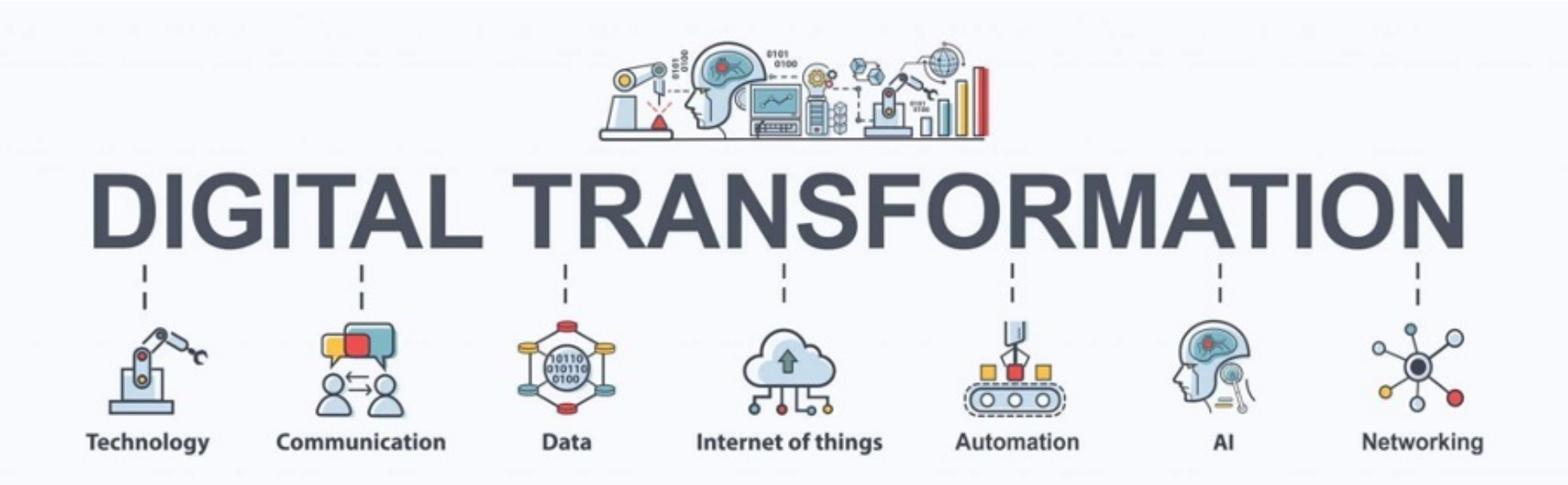
How Does Government Balance Innovation with Security?

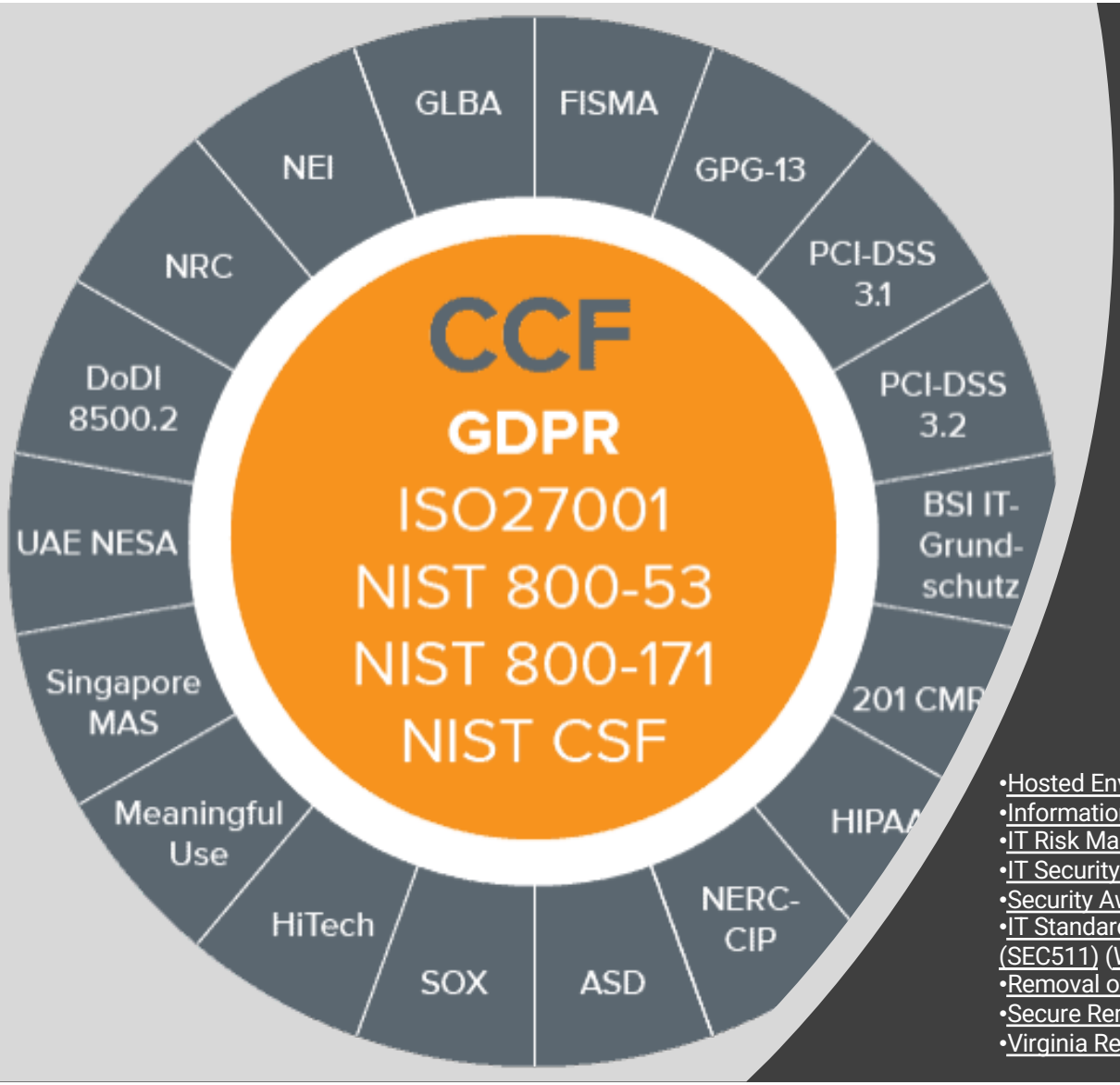


DIGITAL TRANSFORMATION

Cyber the new Transformation

IT Modernization





SEC 525

Adherents to Compliance Drives Protection

- Hosted Environment Information Security Standard (SEC525) (Word version)
- Information Security Standard (SEC501) (Word version)
- IT Risk Management Standard (SEC520) (Word version)
- IT Security Audit Standard (SEC502) (Word version)
- Security Awareness Training Standard (SEC527-00.3) (Word version)
- IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511) (Word version)
- Removal of Commonwealth Data from Electronic Media Standard (SEC514)
- Secure Remote Access to Online Court Documents Standard (SEC503-02.2)
- Virginia Real Property Electronic Recording Standard (SEC505)

Why the U.S. Government is Moving to Cloud Computing

CULTURE | GEAR | IDEAS | SCIENCE | SECURITY | TRANSPO

PARTNER CONTENT SUJATHA PEREPA, IBM

WHY THE U.S. GOVERNMENT IS MOVING TO CLOUD COMPUTING

Image: opensourceway/Flickr

It's no secret that cloud computing is transforming businesses across industries and creating a paradigm shift by delivering hosted services through the internet with unabated cost benefits and business innovation. But while the private sector is building on cloud computing's myriad benefits, government organizations have also aggressively begun to capitalize on them.

As an IBM solution architect and a trusted advisor to many of our government sector customers, I've seen how the financial constraints of the past five years have deeply affected how agencies deploy their solutions. These agencies are pressed to seek optimized business

Government Increases Its Adoption of Cloud Computing both Private and Public

The Government Issued Cloud Policies to Increase Progression

The federal government has issued a **"cloud first"** policy as a part of the Office of Management and Budget's 25-point plan to reform federal information technology management. The policy was described by federal CIO Vivek Kundra during a December 9, 2010, presentation. This cloud-first policy was presented as an important aspect of government reform efforts in order to achieve operational efficiencies by adopting "light" technology and shared services.

As of June 2019, the Federal Cloud Computing Strategy — **Cloud Smart** — is a long-term, high-level strategy to drive cloud adoption in Federal agencies. This was the first cloud policy update in seven years, offering a path forward for agencies to migrate to a safe and secure cloud infrastructure.

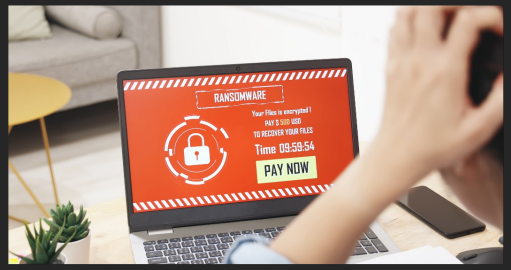
CYBER EXPLOTATIONS!

US Government High Profile Cyber Attacks

- **Ransomware**
  - Hackers targeted U.S. city and county governments with 79 ransomware attacks in 2020, a 35 percent decrease in the number of ransomware attacks counted in 2019 but still a major impact to some 71 million people. The average ransom demanded in 2020 from governmental related organizations was $570,857, with over $1.75 million actually paid to hackers.
- **Log4j**
  - The original Apache Log4j vulnerability (CVE-2021-44228), also known as Log4Shell, is a cybersecurity vulnerability on the Apache Log4j 2 Java library. This security flaw is a Remote Code Execution vulnerability (RCE) - one of the most critical security exposures. Jun 5, 2022
- **SolarWinds**
  - The SolarWinds supply chain attack is a global hack, as threat actors turned the Orion software into a weapon gaining access to several government systems and thousands of private systems around the world. Jun 16, 2021

The Government Strategy Has Changed

IT Modernization for Federal Cybersecurity by Design



THE WHITE HOUSE

Administration Priorities COVID Plan Briefing Room Español MENU

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

EXECUTIVE OFFICE OF THE PRESIDENT
WASHINGTON, D.C. 20503

July 22, 2022

M-22-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: SHALANDA D. YOUNG
DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET

CHRIS INGLIS
NATIONAL CYBER DIRECTOR

SUBJECT: Administration Cybersecurity Priorities for the FY 2024 Budget

US Government Strategy

- **Increase Cyber Security Poster**
  - The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
  - The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
- **Cybersecurity Viewed as National Security**
- Increase IT Modernization to leverage **cloud services**
- **Develop a plan to implement Zero Trust Architecture**, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them

What Is Zero Trust?

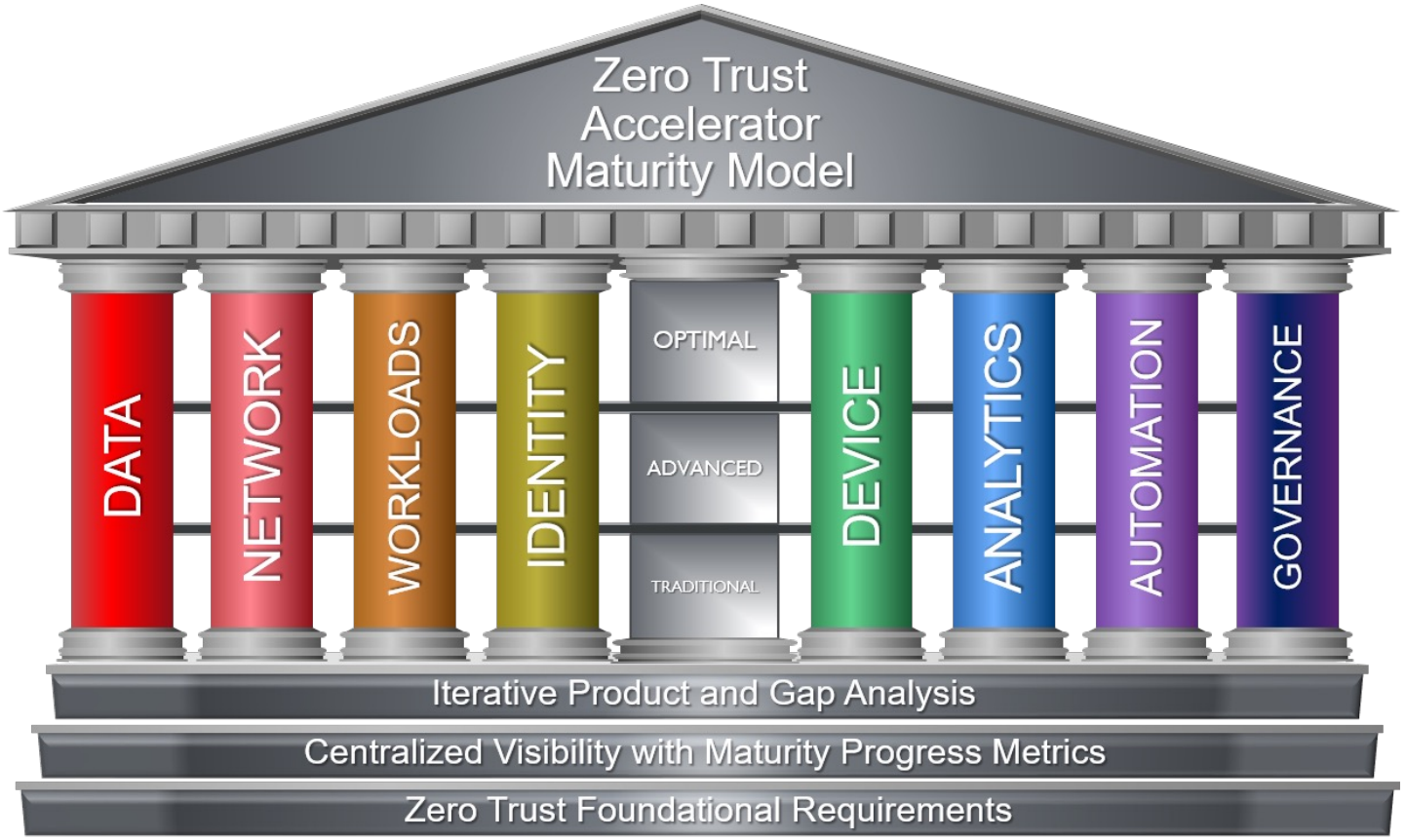
- The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following operative definition of zero trust and ZTA:
  - Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
  - ZTA is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.

What Is Zero Trust?

- Gartner summarized the definitions of Zero Trust from NIST SP 800-207:
  - **Zero Trust** is a cybersecurity paradigm focused on resource protection and the premise the **trust is never granted implicitly but must be *continually evaluated***.
  - A **Zero Trust Strategy** is a systematic approach to **replace implicit trust with adaptive trust** across all of IT.
- In short,
  - We use data to **enrich our adaptive decision making processes** (*continual evaluation*).

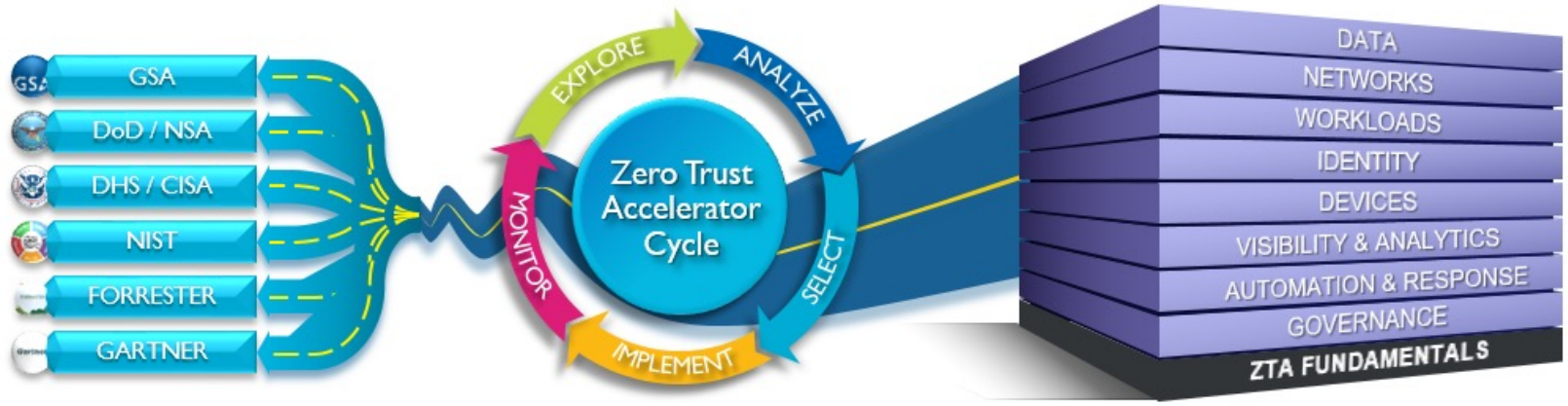
Advancing the Maturity Model

SAIC's Advanced ZT Merged Maturity Model



The maturity model provides a combined picture to address guidance from all Federal and Commercial Models of Zero Trust.

Zero Trust Accelerator's Repeatable Maturity Cycle

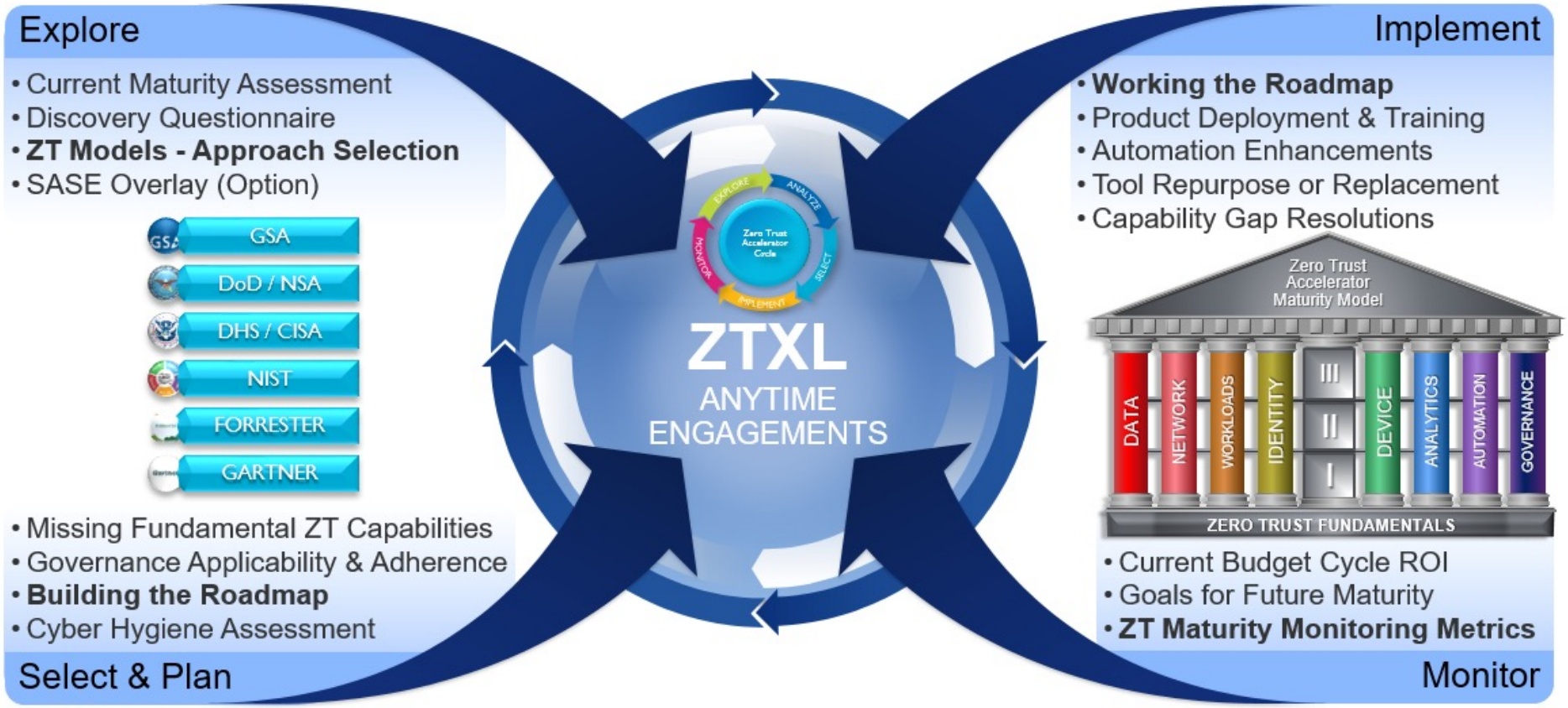


A Phased Approach to Meeting Future Zero Trust Requirements

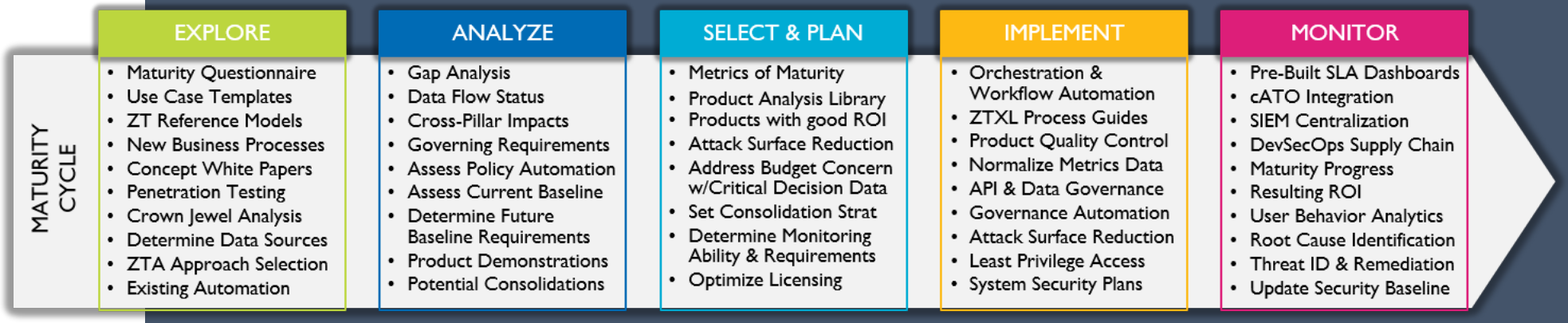
MATURITY CYCLE

EXPLORE	ANALYZE	SELECT & PLAN	IMPLEMENT	MONITOR
• Maturity Questionnaire • Use Case Templates • ZT Reference Models • New Business Processes • Concept White Papers • Penetration Testing • Crown Jewel Analysis • Determine Data Sources • ZTA Approach Selection • Existing Automation	• Gap Analysis • Data Flow Status • Cross-Pillar Impacts • Governing Requirements • Assess Policy Automation • Assess Current Baseline • Determine Future Baseline Requirements • Product Demonstrations • Potential Consolidations	• Metrics of Maturity • Product Analysis Library • Products with good ROI • Attack Surface Reduction • Address Budget Concern w/Critical Decision Data • Set Consolidation Strat • Determine Monitoring Ability & Requirements • Optimize Licensing	• Orchestration & Workflow Automation • ZTXL Process Guides • Product Quality Control • Normalize Metrics Data • API & Data Governance • Governance Automation • Attack Surface Reduction • Least Privilege Access • System Security Plans	• Pre-Built SLA Dashboards • cATO Integration • SIEM Centralization • DevSecOps Supply Chain • Maturity Progress • Resulting ROI • User Behavior Analytics • Root Cause Identification • Threat ID & Remediation • Update Security Baseline

ZTXL Phase Engagements
– Start Anywhere –



ZTXL Maturity Lifecycle Phase Breakdowns & Examples



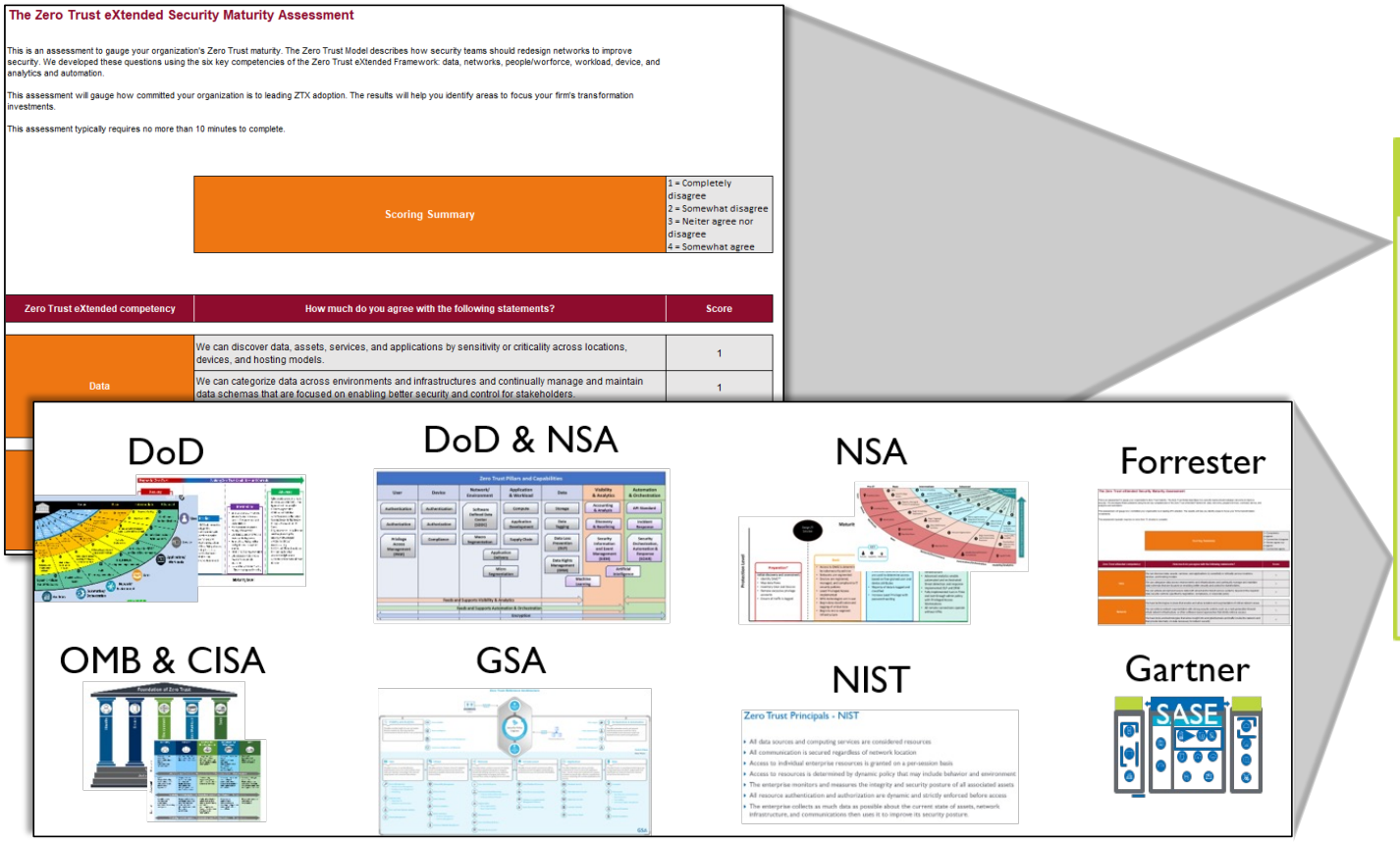
SAIC

ZTXL Maturity Lifecycle Explore Phase

SAIC

Phase 1 : Explore

- Zero Trust education, Use Cases, and discovery tools help determine your zero trust strategy, while also helping us learn about your unique existing environment and technologies.



EXPLORE

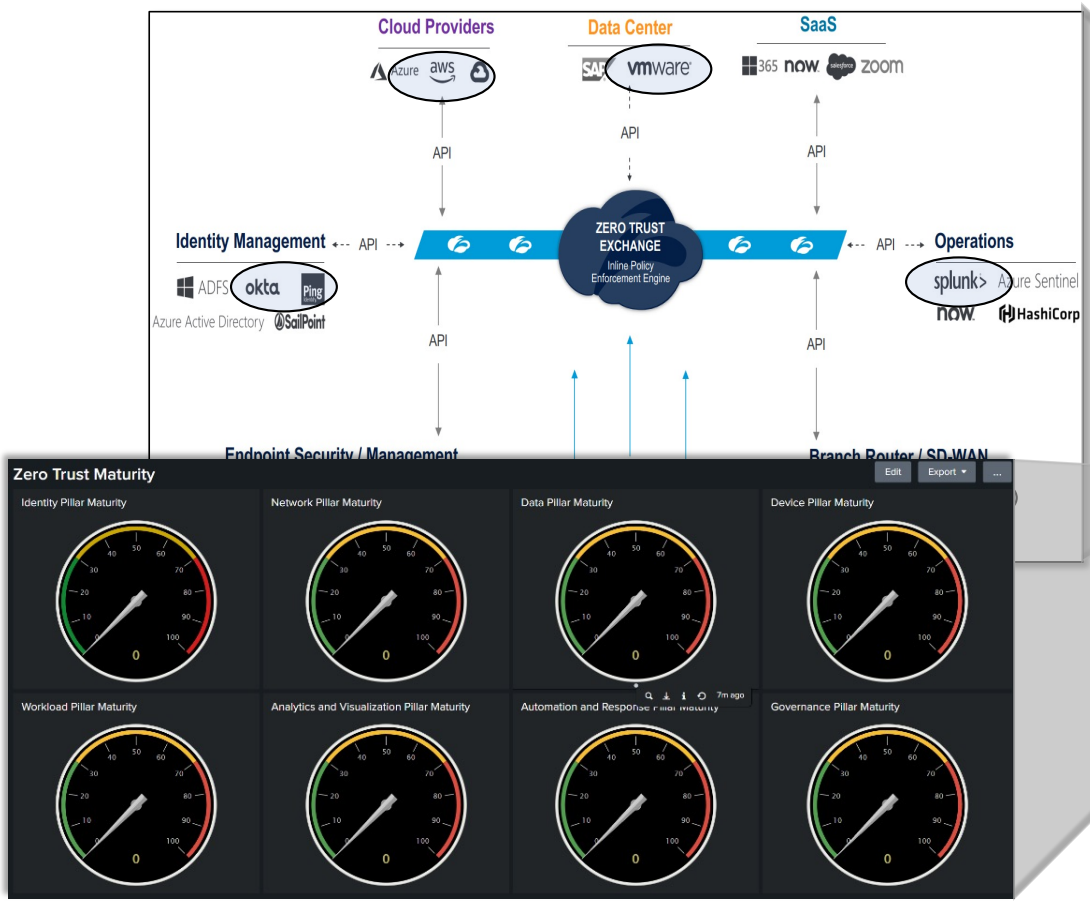
- Maturity Questionnaire
- Use Case Templates
- ZT Reference Models
- New Business Processes
- Concept White Papers
- Penetration Testing
- Crown Jewel Analysis
- Determine Data Sources
- ZTA Approach Selection
- Existing Automation

ZTXL Maturity Lifecycle Analyze Phase

SAIC

Phase II : Analyze

- The data gathered during the Explore phase is then analyzed to identify missing ZT fundamentals, current maturity levels, data flows, and the impact of your unique governance requirements.



ANALYZE

- Gap Analysis
- Data Flow Status
- Cross-Pillar Impacts
- Governing Requirements
- Assess Policy Automation
- Assess Current Baseline
- Determine Future Baseline Requirements
- Product Demonstrations
- Potential Consolidations

ZTXL Maturity Lifecycle
Select & Plan Phase

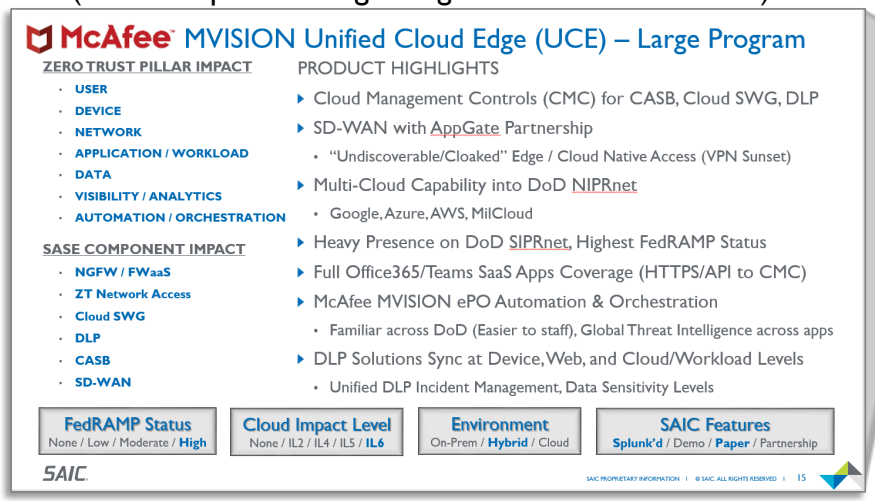
SAIC

Phase III : Select & Plan

- ZTXL saves time and labor needed to ROADMAP required maturity improvements.

- SAIC Innovation's Product Analysis Library (PAL) has compiled data on 100+ competitive vendors in the Zero Trust project space by:
  - Impacted Zero Trust Pillars & SASE Components
  - Product Highlights & Capability Gaps
  - FedRAMP Status
  - Cloud Impact Level
  - Deployable Environments
  - Analytic Capability
  - Demo Availability
  - White Papers Available
  - Partnership Services, Support, and Licensing Discounts

(PAL Example of a Large Program Zero Trust Solution)

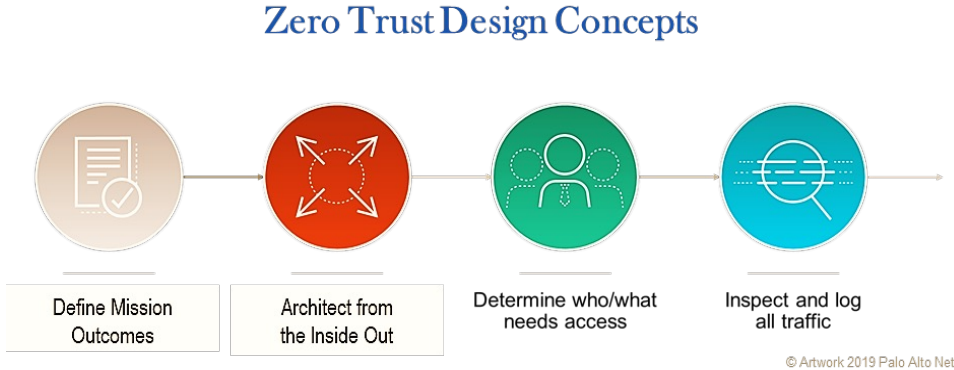


SELECT & PLAN

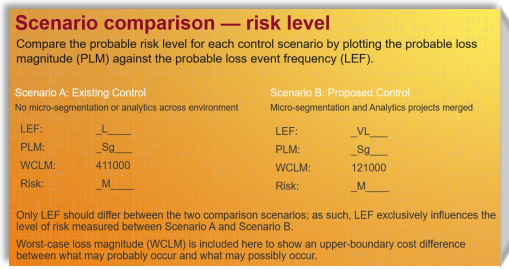
- Metrics of Maturity
- Product Analysis Library
- Products with good ROI
- Attack Surface Reduction
- Address Budget Concern w/Critical Decision Data
- Set Consolidation Strat
- Determine Monitoring Ability & Requirements
- Optimize Licensing

Phase III : Select & Plan

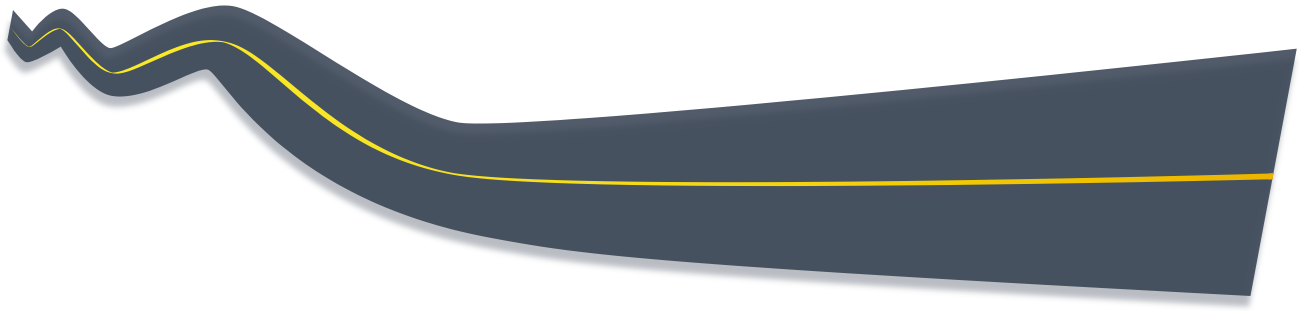
- Selection Methodology based upon clear Technology and Governance Requirements to **QUALIFY PRODUCTS**



- Risk Reduction calculations help customers **QUANTIFY VALUE** by project scenario and other fiscal metrics.



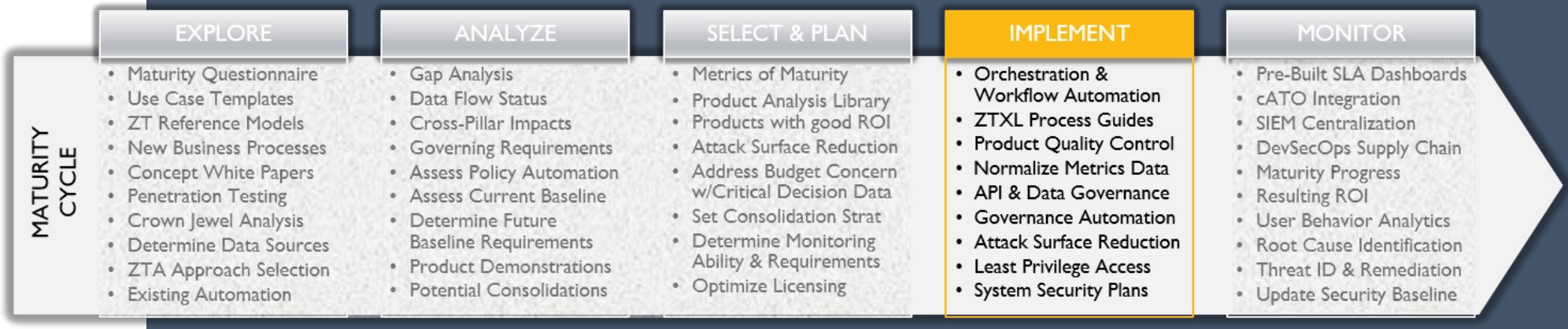
- The final planning outcome is to **BUILD THE ROADMAP**



SELECT & PLAN

- Metrics of Maturity
- Product Analysis Library
- Products with good ROI
- Attack Surface Reduction
- Address Budget Concern w/Critical Decision Data
- Set Consolidation Strat
- Determine Monitoring Ability & Requirements
- Optimize Licensing

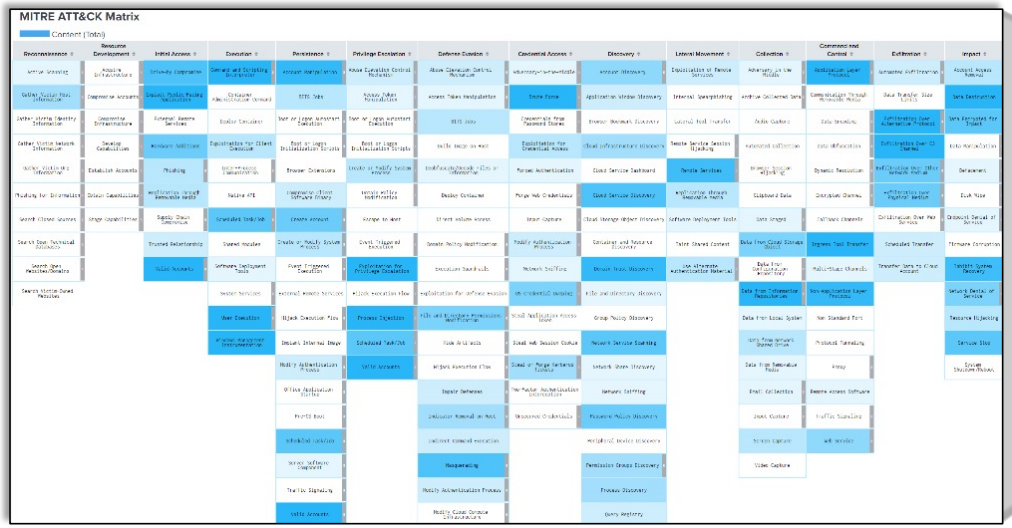
ZTXL Maturity Lifecycle Implement Phase



SAIC

Phase IV : Implement

- Implementation is about *more* than the ROADMAP developed in phase III.
  - The technology changes made during implementation
    - Reduce Attack Surface – mapped to the MITRE ATT&CK Matrix (below)
    - Improve ATO System Security Plans due to **reducing or mitigating risk**
    - Most Important to Zero Trust, the tools provide enriched data for Adaptive Decision Making
      - Adaptive Decision Making helps to further **remove Implicit Trust from your environment**.

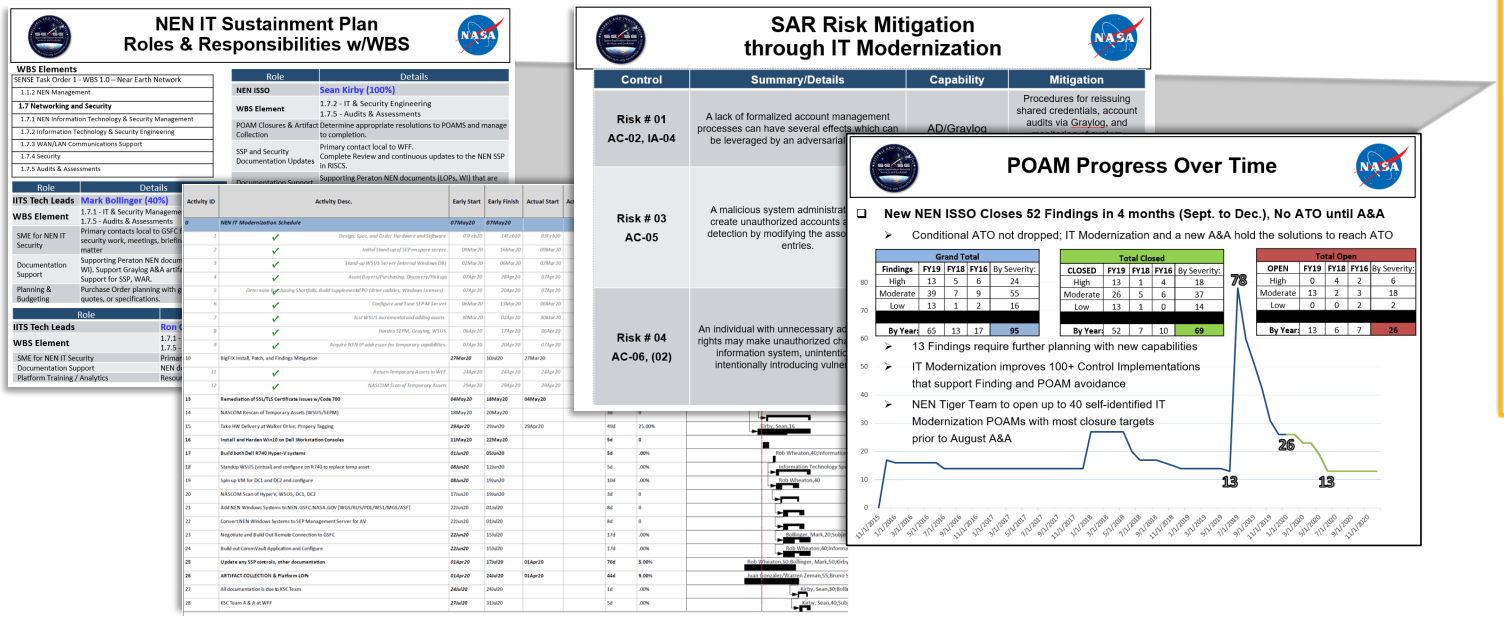


IMPLEMENT

- Orchestration & Workflow Automation
- ZTXL Process Guides
- Product Quality Control
- Normalize Metrics Data
- API & Data Governance
- Governance Automation
- Attack Surface Reduction
- Least Privilege Access
- System Security Plans

Phase IV : Working the ROADMAP

- Weekly briefing to keep customers up-to-date on roadmap progress:
  - POCs aligned with their Areas of Responsibility
  - Resource Loaded Schedules with Milestone State
  - Risk Mitigation Impacts by new ZT Capabilities associated with NIST Controls
  - Zero Trust Maturity Metrics, POAM Impacts, and SSP Updates.



IMPLEMENT

- Orchestration & Workflow Automation
- ZTXL Process Guides
- Product Quality Control
- Normalize Metrics Data
- API & Data Governance
- Governance Automation
- Attack Surface Reduction
- Least Privilege Access
- System Security Plans

ZTXL Maturity Lifecycle Monitor Phase

SAIC

Phase V : Monitor

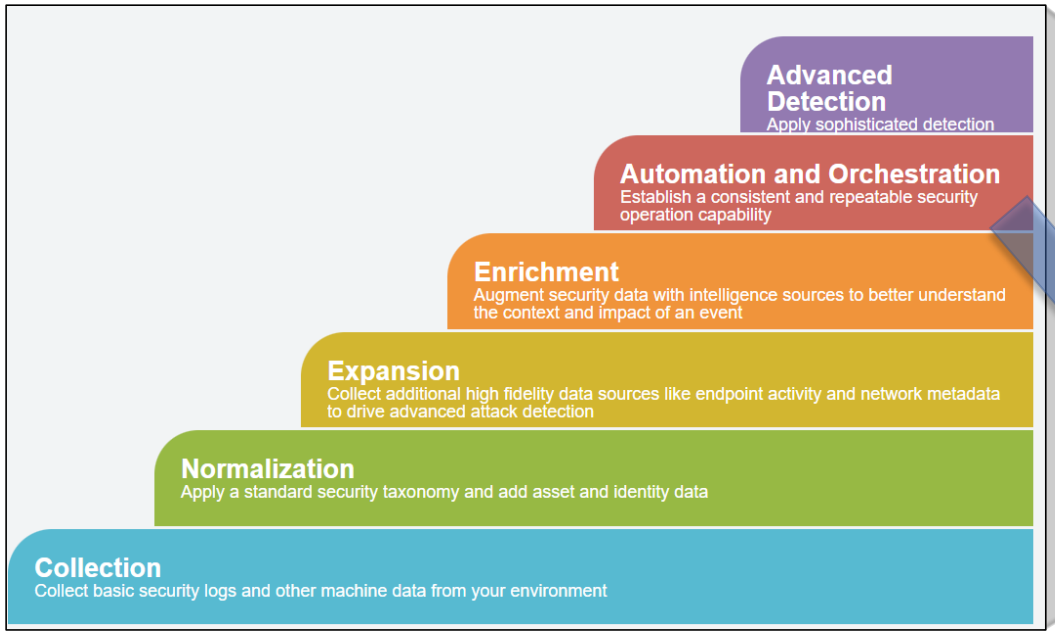
Zero Trust Requires Continuous Monitoring

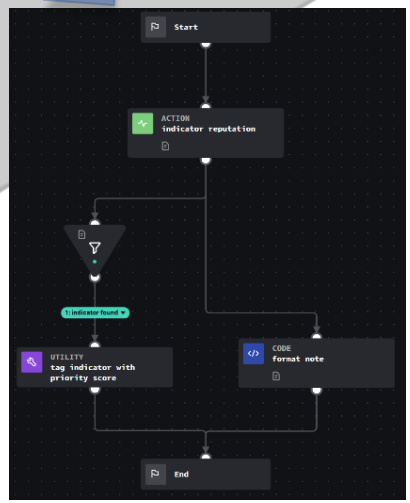
NIST: Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.

Gartner: Zero trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk/trust levels based on identity and context supported by security infrastructure that adapts to risk-optimize the organization's security posture.

Phase V : Monitor (How well are you using data?)

- Analytic Maturity is critical to Automation/Orchestration for advanced Zero Trust decision making.





MONITOR

- Pre-Built SLA Dashboards
- cATO Integration
- SIEM Centralization
- DevSecOps Supply Chain
- Maturity Progress
- Resulting ROI
- User Behavior Analytics
- Root Cause Identification
- Threat ID & Remediation
- Update Security Baseline

- Increased SIEM Maturity leads to SOAR integration.
  - Security Orchestration and Automated Response
    - SOAR integration leads to enriched ZT decision making.

Benefits of ZTXL and the Maturity Model

- Zero Trust Accelerator
  - **Saves customers Time and Labor**
    - Pre-Built Tools and Analytic Templates, MITRE mapping, Data Use Case Library
    - ZT Product Analysis Library saves time exploring technology to fill fundamental ZT gaps fast
    - Direct Mapping from ZT to NIST Controls to minimize ATO impact and maximize POAM resolution
  - **Cuts through requirements,** overlaying them on ZT Controls
    - Solve for multiple governance requirements simultaneously with Governance Overlays
  - **Provides a long-term Roadmap future FY budget planning**.
    - Know where and when Governance expectations and required Risk reductions will be met.
    - Accurate POAM planning leads to faster ATOs, *and Continuous ATO Options*.
  - **Quantifies the entire journey to Zero Trust maturity** with ROI and ZT Maturity Analytics.
    - The investments in ZTXL and new technologies have measurable Risk Impacts, reflected back to the dollars spent.

Discussion

Shawn Kingsberry, SAIC, VP Cybersecurity